UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/721,753	11/26/2003	Choon B. Shim	QOVI-002/00US	3938

7590 02/22/2008

ATTN: Patent Group
COOLEY GODWARD LLP
One Freedom Square, Reston Town Center
11951 Freedom Drive
Reston, VA 20190-5656

EXAMINER	
TRAORE, FATOUMATA	
ART UNIT	**PAPER NUMBER**
2136	

MAIL DATE	DELIVERY MODE
02/22/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/721,753	SHIM ET AL.	
	Examiner	Art Unit	
	FATOUMATA TRAORE	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 November 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the amendment filed November 29th, 2007. Claims 1-16 and 21 have been amended; Claims 1-22 are pending and have been considered below.

Claim Objections

2. In light to the amendment of claims 1, 3 and 6, the objection to the claims has been withdrawn.

Response to Arguments

3. Applicant's arguments filed November 29th, 2007 have been fully considered but they are not persuasive.

Regarding claim 1 applicant argued on page 9 of the reply that "(emphasis added) (Nagaoka et al., abstract.) As emphasized above, Nagaoka et al. discloses a "firewall which is interposed between the server and the network." By contrast, amended claim 1 discloses "configuring a ropj.9_~ server outside the first firewall." Further, the server alluded to in Nagaoka et al. is a "WWW server" (see Col. 7, lines 1-20.), and not the proxy server of amended claim 1". In reply the examiner submits that Crichton et al discloses the newly added feature of claim 1(see column 2, lines 32-55; column 4, lines 51-67; Fig. 4, item 26) (***middle server or proxy outside the two firewalls).*** Therefore the examiner submits that the combined teaching of Nagaoka et al and Crichton et al disclose each and every feature of amended claim 1. As claims 2 and 7 depend upon claim 1, claims 2 and 7 are not allowable.

Regarding claim 9, applicant argued on page 10 of the reply that "In contrast to Nagaoka et al., the proxy server is "located outside the first fire wall." Further, as amended claim 9 provides, this proxy server may "aggregate and store performance data provided by the first control unit.". The examiner respectfully disagree and submit that that Crichton et al discloses the newly added feature of claim 1(see column 2, lines 32-55; column 4, lines 51-67; Fig. 4, item 26) (***middle server or proxy outside the two firewall,*** Crichton et al further discloses that the proxy server may aggregate and store performance data provided by the first control unit(see Fig .5 discloses the newly added feature of claim 9(see column 8, lines 23-53; Fig. 5). Therefore, the examiner submits that the combined teaching of Nagaoka et al and Crichton et al disclose each and every feature of amended claim 9. As claim 11 depend upon claim 9, claim 11 is not allowable.

Regarding claim 12, the argument is mood in view of the new ground of rejection.

Regarding claims 16, 18, 19 and 21, the argument is mood in view of the new ground of rejection.

Regarding Claim 3, applicant argued that "Claim 3 discloses in its preamble "configuring the first control unit." In contrast, Brownell discloses, inter alia, "At step 430, tunnel configuration data is generated. Tunnel configuration data describes the tunnels through which connections may be established for a particular user." (emphasis added) (See Col. 11, line 30-33.) The configuration described in the preamble for claim 3 is distinct from the configuration occurring in the portion of Brownell cited by the Examiner". The examiner respectfully disagrees and submits that Crichton et al

discloses each and every element of the claim and further discloses “wherein configuring the first control unit includes: receiving the proxy server identification information (column 6, liness47-63); generating an access key in the first control unit (column6, lines 63-65); and sending the access key and the identification information to the proxy server (column 7, line 57 to column 8 line 24). Therefore, the examiner submits that the combined teaching of Nagaoka et al and Crichton et al disclose each and every feature of amended claim 3. As claims 4-6 depend upon claim 3, claims 4-6 are not allowable.

Regarding claim 8, applicant argued” further, amended claim 8 discloses "connecting between the proxy server and a console, the console being inside the second firewall, the connecting using an IP address facing inside the second firewall." The Examiner cited portion of Brownell (e.g., Col. 4, lines 30-55. Fig. 1) is silent as to the case of the proxy server and the console being inside a firewall”. The examiner submits that the above feature is disclosed by Crichton et al (see Fig. 10).

Regarding Claims 13-15, 17, 20, 21 and 22, the argument is mood in view of a new ground of rejection.

There is no new ground of rejection when the basic thrust of the rejection remains the same. See In re Kronig, 539 F.2d 1300, 1302-03, 190 USPQ 425, 426-27 (CCPA 1976) To the extent that the response to the applicant's arguments may have mentioned new portions of the prior art references, which were not used in the prior office action, this does not constitute new a new ground of rejection. It is clear that the prior art reference is of record and has been considered entirely b' applicant. See In re Boyer, 363 F.2d

455,458 n.2,150 USPQ 441,444, n.2 (CCPA 1966) and In re Bush, 296 F.2d 491,496, 131 USPQ 263,267 (CCPA 1961).

The mere fact that additional portions of the same reference may have been mentioned or relied upon does not constitute new ground of rejection. In re Meinhardt, 392, F.2d 273,280, 157 USPQ 270, 275 (CCPA 1968). Accordingly, this office action is being made final.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nagaoka et al (US 6,651,174) in view of Crichton et al (US 6,104,716).

Claim 1: Nagaoka et al discloses a method for remotely controlling a network comprising:

i. Configuring a first control unit inside a first firewall (column 7, lines 1-20 and FIG. 1);

ii. Configuring a proxy server outside the first firewall (column 7, lines 1-20 and FIG. 1); and

iii. Establishing a session between the first control unit and the proxy server, wherein establishing the session is executed using an access key (column 7, lines 1-20 and FIG. 1).

But, does not explicitly disclose that the firewall is interposed between the proxy server and the network. However, Crichton et al discloses a lightweight secure tunneling protocol, which further discloses that the firewall is interposed between the proxy server and the network(middle server or proxy server outside the two firewalls) (column 2, lines 32-55; column 4, lines 51-67; Fig.4, item 26). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Nagaoka et al such as to interpose the firewall. One would have been motivated to do so in order to enable authentication between entities in communication.

Claim 2: Nagaoka et al and Crichton et al disclose a method for remotely controlling a network as in claim 1, and Nagaoka et al further discloses a step of configuring a second control unit inside a second firewall, the proxy server being outside the second firewall (column 2, lines 2-20 FIG 1, FIG. 4).

Claim 3: Nagaoka et al and Crichton et al disclose a method for remotely controlling a network as claim 1 above, which further discloses a step of receiving the proxy server identification information (FIG 3, FIG 4) and a step of sending the access key and the identification information to the server (FIG 3, FIG 4). Although it is clear that the teaching of Nagaoka et al inherently involve generating access key in the first control unit, Nagaoka et al was silent about the

step generating access key during the authentication process. However, generating access key in the first control unit was know and commonly practiced in the art at the time the invention was made. Further as evidence by the teaching of Crichton et al further indicated receiving the proxy server identification information (column 6, liness47-63); generating an access key in the first control unit (column6, lines 63-65); and sending the access key and the identification information to the proxy server (column 7, line57 to column 8 line 24) (column 11 line 30-65 and FIG. 4, block 430). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Nagaoka et al such as to include the step of generating access key. One would have been motivated to do so in order to enable authentication between entities in communication.

Claims 4, 10: Nagaoka et al and Crichton et al disclose a method and system for remotely controlling a network as claims 3 and 9 above, and Crichton et al further discloses that the step of receiving the proxy server identification information includes receiving a proxy server host name, a proxy server IP address, and a proxy server port number (column 6, lines 55-65). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Nagaoka et al such as to add a step of receiving information. One would have been motivated to do so in order to enable authentication between entities in communication.

Claim 5: Nagaoka et al and Crichton et al disclose a method for remotely

controlling a network as claim 3 above, and Crichton et al further discloses that the step of receiving the proxy server identification information includes inquiring the proxy server from the first control unit to obtain the server IP address (column 6, lines 55-65). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Nagaoka et al such as to add a step of receiving information. One would have been motivated to do so in order to enable authentication between entities in communication.

Claim 6: Nagaoka et al and Crichton et al disclose a method and system for remotely controlling a network as claim 1 above, and Nagaoka et al further discloses a step of receiving the first control unit identification information (FIG 3, FIG 4) and a step exchanging a validation message between the first control unit and the server (FIG 3, FIG 4). Although it is clear that the teaching of Nagaoka et al inherently involve storing identification information and adding the control unit to the remote device, Nagaoka et al was silent about the step storing identification information and adding the control unit to the remote device. However, storing the first control unit identification information and adding the first control unit as a first remote device was know and commonly practiced in the art at the time the invention was made. Further as evidence by the teaching of Crichton et al a further discloses a step of storing the first control unit identification information in the server and a step of adding the first control unit as a first remote device (column 8, lines 23-53; Fig. 5). Therefore, it would have

been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Nagaoka et al such as to include the step of generating access key. One would have been motivated to do so in order to enable authentication between entities in communication.

Claim 7: Nagaoka et al and Crichton et al disclose a method for remotely controlling a network as in claim 1above, and further discloses a step of establishing a session between the first control unit and the proxy server includes coupling through a second firewall, the proxy server being inside the second firewall (column 6, lines 13-51).

Claim 8: Nagaoka et al and Crichton et al disclose a method for remotely controlling a network as claim 7 above, and Crichton et al further discloses 7, further comprising connecting between the proxy server and a console, the console being inside the second firewall, the connecting using an IP address facing inside the second firewall (Fig. 10). Therefore it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the teaching of Nagaoka et al such as to establish the connection between the proxy server and a second firewall. One would have been motivated to do so in order to prevent attempts to gain access critical data.

Claim 9: Nagaoka et al discloses a communication system comprising:

i. A first enterprise network (column 7, lines 1-20 and FIG. 1, FIG 5);

ii. A first control unit coupled to the first enterprise network (column 7, lines 1-20 and FIG. 1, FIG 5);

iii. A first firewall coupled to the first control unit (column 7, lines 1-20 and FIG. 1, FIG 5);

iv. A public network (FIG 5); and

But does not explicitly discloses a proxy serve, located outside the first firewall, coupled to the public network, the first control unit being configured with proxy server information, the proxy server being configured with first control unit information, the first control unit being further configured to send a first access key to the proxy server, the first control unit and the proxy server configured to establish a communication session based on the first access key, the proxy server to aggregate and store performance data provided by the first control unit. However, Crichton et al discloses a lightweight secure tunneling protocol, which further discloses that discloses a proxy serve, located outside the first firewall, coupled to the public network (column 2, lines 32-55; column 4, lines 51-67; Fig.4, item 26), the first control unit being configured with proxy server information, the proxy server being configured with first control unit information, the first control unit being further configured to send a first access key to the proxy server(column 4, lines 35-55), the first control unit and the proxy server configured to establish a communication session based on the first access key the proxy server to aggregate and store performance data provided by the first control unit9column 8, lines 23-53; Fig.5). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Nagaoka et al such as to have a proxy server outside the first firewall

and to store performance data. One would have been motivated to do so in order to enable authentication between entities in communication.

Claim 11: Nagaoka et al and Crichton et al disclose a communication system as in claim 9 above, and Nagaoka et al further comprising:

i. A second firewall coupled to the public network (column 7, lines 21-31 and FIG 1, FIG 2);

ii. A second control unit coupled to the second firewall (column 7, lines 21-31 and FIG 1, FIG 2); and

iii. A second enterprise network coupled to the second control unit, the second control unit being configured with proxy server information, the proxy server being configured with second control unit information, the second control unit being further configured to send a second access key to the proxy server, the second control unit and the server configured to establish a communication session based on the second access key (FIG 7A, FIG 7B).

6. Claims 16, 18, 19 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Crichton et al (US 6,104,716) in view of Lomet et al (US 6,182,086).

Claim 16: Crichton et al discloses a system for secure communication tunneling over the Internet comprising:

i. A first console configured to generate at least one console request message (FIG. 5);

ii. A proxy server coupled to the first console, the proxy server configured to pool the at least one request (FIG. 5), and to provide access from at least one console to the first control unit;

iii. A first firewall coupled to the proxy server (FIG. 3); and

iv. A first control unit coupled to the first firewall, the first control unit configured to receive the at least one request from the proxy server, the first control unit further configured to output at least one response corresponding to the at least one request to the proxy server, the proxy server configured to output the at least one response to the first console (column 5, lines 45-60, and FIGs. 3, 4, 5-8).

But does not explicitly discloses that he console request message including at least one of a request for network management data, a request for internet Protocol (IP)-Private Branch Exchange (PBX), or a request for status information. However, Lomet et al discloses a client server computer system, which further discloses that he console request message including at least one of a request for network management data, a request for internet Protocol (IP)-Private Branch Exchange (PBX), or a request for status information(column 9, lines 32-40). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Crichton et al such as to include in the console message at least one of a request for network management data, a request for internet Protocol (IP)-Private Branch Exchange (PBX), or a request for status information. One would have been motivated to do so in order to enable

authentication between entities in communication.

Claim 18: Crichton et al and Lomet et al disclose a system for secure communication tunneling over the Internet as in claim 16 above, and Crichton et al further discloses:

i. A second firewall coupled to the proxy server (column 3, line 28 to column 6 line 9); and

ii. A second control unit, the second control unit coupled to the second firewall, the second control unit configured to receive the at least one request from the proxy server, the second control unit further configured to output at least one response corresponding to the at least one request to the proxy server, the proxy server configured to output the at least one response to the first console (column 5 line 61 to column 6 line 38, column 10 lines 35-53FIG 5).

Claim 19: Crichton et al and Lomet et al disclose a system for secure communication tunneling over the Internet as in claim 16 above, and Crichton et al further discloses:

i. A client request handler for receiving a client request from the first console (column 7, lines 10-15, and FIG 5);

ii. A shared request object pool coupled to the client request handler, the shared request

object pool configured to store the at least one request (column 8, lines 24-52, and FIG. 8); and

iii. A server request handler coupled to the shared request object pool, the server request handler configured to read the at least one request from the shared request object pool, the server request handler configured to send the at least one request to the first control unit, the server request handler configured to receive the at least one response, the server request handler configured to output the at least one response to the first console (column 7, line 58 to column 8 line 23, and FIG 7).

Claim 21: Crichton et al discloses a system for secure communication tunneling over the Internet comprising:

i. Receiving a console request message from a console, he console request message including at least one of a request for network management data, a request for Internet Protocol (IP)-Private Branch Exchange (PBX), or a request for status information (FIG. 8);

ii. Creating a request object (FIG. 8);

ii. Adding the request object to a pool (FIG. 8); and

iii. Notifying a control unit of the request object (FIG. 8).

But does not explicitly discloses that he console request message including at least one of a request for network management data, a request for internet Protocol (IP)-Private Branch Exchange (PBX), or a request for status information. However, Lomet et al discloses a client server computer system, which further discloses that he console request message including at least one of a request for network management data, a request for internet Protocol (IP)-Private Branch Exchange

(PBX), or a request for status information(column 9, lines 32-40). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Crichton et al such as to include in the console message at least one of a request for network management data, a request for internet Protocol (IP)-Private Branch Exchange (PBX), or a request for status information. One would have been motivated to do so in order to enable authentication between entities in communication.

7. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Nagaoka et al (US 6,651,174) in view of Beurket et al (US 6,360,273).

Claim 12: Nagaoka et al discloses a communication system comprising:

b. A first enterprise network (column 7, lines 1-20 and FIG. 1, FIG 5);

c. A first control unit coupled to the first enterprise network (column 7, lines 1-20 and FIG. 1, FIG 5);

d. A first firewall coupled to the first control unit (column 7, lines 1-20 and FIG. 1, FIG 5);

e. A public network (FIG 5); and

But does not explicitly disclosed a proxy server that includes at least one of a client request handler, a shared request object pool, or a server request handler. However, Beurket et al discloses system for collaborative transformation, which further discloses that proxy server that includes at least one of a client request handler, a shared request object pool, or a server request handler(Fig. 2, item

1129 and 230). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Nagaoka et al such as to include at least one of a client request handler, a shared request object pool, or a server request handler in the proxy server. One would have been motivated to do so in order to enable authentication between entities in communication.

8. Claims 13-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nagaoka et al (US 6,651,174) in view of Beurket et al (US 6,360,273) in further view of Crichton et al (US 6,104,716).

Claim13: Nagaoka et al and Beurket et al disclose a method and system for remotely controlling a network as claim 12 above, and Nagaoka et al further discloses a step of receiving the first control unit identification information (FIG 3, FIG 4) and a step exchanging a validation message between the first control unit and the server (FIG 3, FIG 4). Although it is clear that the teaching of Nagaoka et al inherently involve storing identification information and adding the control unit to the remote device, Nagaoka et al was silent about the step storing identification information and adding the control unit to the remote device. However, storing the first control unit identification information and adding the first control unit as a first remote device was know and commonly practiced in the art at the time the invention was made. Further as evidence by the teaching of Crichton et al a further discloses a step of storing the first control unit

identification information in the server and a step of adding the first control unit as a first remote device (column 8, lines 23-53; Fig. 5). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Nagaoka et al and Beurket et al such as to include the step of generating access key. One would have been motivated to do so in order to enable authentication between entities in communication.

Claim 14: Nagaoka et al , Beurket et al and Crichton et al disclose a system for remotely controlling a network as claim 13 above, and Nagaoka et al further discloses:

i. A second firewall coupled to the public network (column 7, lines 21-31 and FIG 1, FIG 2);

ii. a second control unit means coupled to the second firewall (column 7, lines 21-31 and FIG 1, FIG 2); and

iii. a second enterprise network coupled to the second control unit, the second control unit means configured to receive proxy server means identification information, generate access key in the first control unit means, and send the access key and the identification information to the proxy server means (FIG 7A, FIG 7B).

Claim 15: Nagaoka et al, Beurket et al and Crichton et al disclose a system for remotely controlling a network as claim 14 above, Nagaoka et al further discloses a step of receiving first control unit identification information (FIG 3, FIG 4) and a step exchanging a validation message between the first control unit and the

server (FIG 3, FIG 4). Although it is clear that the teaching of Nagaoka et al inherently involve storing identification information and adding the control unit to the remote device, Nagaoka et al was silent about the step storing identification information and adding the control unit to the remote device. However, storing the first control unit identification information and adding the first control unit as a first remote device was know and commonly practiced in the art at the time the invention was made. Further as evidence by the teaching of Crichton et al further discloses a step of storing the first control unit identification information in the server and a step of adding the first control unit as a first remote device (column 8, lines 23-53; Fig. 5). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Nagaoka et al and Beurket et al such as to include the step of generating access key. One would have been motivated to do so in order to enable authentication between entities in communication.

9. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Crichton et al (US 6,104,716) in view of Lomet et al (US 6,182,086) in further view of Nagaoka et al (US 6,651,174).

Claim 17: Crichton et al and Lomet et al disclose a system for secure communication tunneling over the Internet as in claim 16 above, while neither of them explicitly discloses a second console coupled a proxy. However, Nagaoka et al discloses a system for remotely controlling a network, which further

discloses a second console coupled to the proxy server, the second console configured to generate at least one other request, the proxy server configured to pool the at least one other request (FIG. 5, FIG. 7B). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Crichton et al and Lomet et al such as to couple a second console with proxy (firewall). One would have been motivated to do so in order to present against unauthorized access.

10. Claims 20, 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Crichton et al (US 6,104,716) in view of Lomet et al (US 6,182,086) in further view of Nelson (US 6,553,422).

Claim 20: Crichton et al and Lomet et al disclose a system for secure communication tunneling over the Internet as in claim 16 above, while neither of them explicitly discloses a step of receiving, writing, reading a request and outputting a response. However, Nelson discloses a reserve http connection for device management, which further performs the steps of:

b. Receiving a client request from the first console (column 4 line11-53, and FIG. 3, FIG. 4);

c. Writing the at least one request (column 60-67);

d. Reading the at least one request (column 4 line11-53, and FIG. 3, FIG. 4);

e. Sending the at least one request to the first control unit (column 4 line11-53, and FIG. 3, FIG. 4);

f. Receiving the at least one response (column 4 line11-53, and FIG. 3, FIG. 4); and

g. Outputting the at least one response to the first console (column 4, line11-53; and FIG. 3, FIG. 4).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Crichton et al and Lomet et al such as to read, send, and output a request. One would have been motivated to do so in order to present against unauthorized access.

Claim 22: Crichton et al and Lomet et al disclose a system for secure communication tunneling over the Internet as in claim 21 above, while neither of them explicitly discloses the step of receiving, writing, reading a request and outputting a response. However, Nelson discloses a reserve http connection for device management, which further performs the steps of:

a. Establishing a data connection with the control unit (column 4 line11-53, and FIG. 3, FIG. 4);

b. Receiving a request from the control unit for the request object (column 4 line11-53, and FIG. 3, FIG. 4);

c. Sending the request object to the control unit (column 4 line11-53, and FIG. 3, FIG. 4);

d. Receiving a response from the control unit based on the request object (column 4 line11-53, and FIG. 3, FIG. 4); and

e. Sending the response to the console (column 4 line11-53, and FIG. 3, FIG. 4).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Crichton et al and Lomet et al such as to read, send, and output a request. One would have been motivated to do so in order to present against unauthorized access.

Conclusion

11. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685. The examiner can normally be reached Monday through Thursday from 7:00 a.m. to 4:00 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nassar G. Moazzami, can be reached on (571) 272 4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-8300. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 270-2685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

FT
Tuesday, February 19th, 2008

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2136